

CRYPTANALYSIS OF ANDRECUT'S PUBLIC KEY CRYPTOSYSTEM

VITALII ROMAN'KOV AND ANTON MENSHOV

1

ABSTRACT. We show that a linear decomposition attack based on the decomposition method introduced by the first author in monography [1] and papers [2], [3], and developed in [4], works by finding the exchanging key in the protocol in [5].

1. INTRODUCTION

In this note we apply a practical deterministic attack on the protocol proposed in [5]. This kind of attack introduced by the first author in [1], [2], [3] and developed in [4] works when the platform objects are linear. It turns out that in this case, contrary to the common opinion (and some explicitly stated security assumptions), one does not need to solve the underlying algorithmic problems to break the scheme, i.e., there is another algorithm that recovers the private keys without solving the principal algorithmic problem on which the security assumptions are based. The efficacy of the attack depends on the platform group, so it requires a specific analysis in each particular case. In general one can only state that the attack is in polynomial time in the size of the data, when the platform and related groups are given together with their linear representations. In many other cases we can effectively use known linear presentations of the groups under consideration. A theoretical base for the decomposition method is described in [4] where a series of examples is presented. The monography [1] solves uniformly many protocols based on the conjugacy search problem, protocols based on the decomposition and factorization problems, protocols based on actions by automorphisms, and a number of other protocols. See also [6] and [7] where the linear decomposition attack is applied to the main protocols in [8], [9], and [10].

In a series of works [11], [12] and [13] (see also [14]) Tsaban presented another general approach for provable polynomial time solutions of computational problems in groups with efficient, faithful representation as matrix groups.

All along the paper we denote by \mathbb{N} the set of all nonnegative integers, and by \mathbb{C} the set of all complex numbers.

¹Supported by RFBR, projects 13-01-00239 and 15-41-04312.

2. ANDRECUT'S KEY EXCHANGE PROTOCOL [5].

In this section, we describe the Andrecut's key exchange protocol proposed in [5]. Firstly we introduce a necessary terminology. Then we will give a cryptanalysis of this protocol.

Let $X \in \mathbb{C}^{n \times n}$ be a complex matrix of size $n \times n$, that is considered as a variable. Let

$$P(X, a) = \sum_{m=1}^M a_m X^m \text{ and } Q(X, b) = \sum_{m=1}^K b_m X^m$$

be two complex polynomials in X uniquely defined by the complex vectors of coefficients $a = (a_0, \dots, a_M)$ and $b = (b_0, \dots, b_K)$.

- Alice chooses the secret vectors $a \in \mathbb{C}^{M_1}$ and $\tilde{a} \in \mathbb{C}^{M_2}$ (Alice's private key).
- Alice randomly generates and publishes the matrix $U \in \mathbb{C}^{n \times n}$ (Alice's matrix public key).
- Bob chooses the secret vectors $b \in \mathbb{C}^{J_1}$ and $\tilde{b} \in \mathbb{C}^{J_2}$ (Bob's private key).
- Bob randomly generates and publishes the matrix $V \in \mathbb{C}^{n \times n}$ (Bob's matrix public key).
- Alice computes and publishes the matrix $A = P(U, a)P(V, \tilde{a})$ (Alice's public key).
- Bob computes and publishes the matrix $B = P(U, b)P(V, \tilde{b})$ (Bob's public key).
- Alice calculates the secret matrix $K_A = P(U, a)BP(V, \tilde{a})$.
- Bob calculates the secret matrix $K_B = P(U, b)AP(V, \tilde{b})$.
- The established secret key is $K = K_A = K_B$.

It is assumed in [5], that the matrices U and V are different to give the non-commutativity assumption $P(U, a)P(V, b) \neq P(V, b)P(U, a)$ and $P(U, \tilde{a})P(V, \tilde{b}) \neq P(V, \tilde{b})P(U, \tilde{a})$. In general, even more strong assumption $UV \neq VU$ is not enough for this non-commutativity.

Also, there is a remark in [5] that the following assumption

$$M_1, M_2, J_1, J_2 \gg n$$

should be satisfied in order to increase the security. But by the classical Cayley-Hamilton theorem every matrix U is a root of its own characteristic polynomial $C(X) = \det(U - X \cdot I_n)$, where I_n is the identity matrix of size $n \times n$. The degree of $C(X)$ is exactly n . Then for any matrix $U \in \mathbb{C}^{n \times n}$ and every matrix polynomial $P(X, a)$ one has $P(U, a) = R(U)$, where $R(X)$ is the remainder after division of the polynomial $P(X, a)$ by $C(X)$. Hence, there is no sense to use in the protocol above polynomials of degrees $\geq n$.

3. CRYPTANALYSIS OF THE ANDRECUT'S KEY EXCHANGE PROTOCOL [5].

We will provide two approaches to cryptanalysis of the protocol described in the previous section. The first one is based on some simple facts from linear algebra and the second one is based on a linear decomposition attack.

As we have seen in the previous section, there is no sense to use values $M_1, M_2, J_1, J_2 \geq n$. Thus we can assume that $M_1 = M_2 = J_1 = J_2 = n - 1$. Consider the linear systems

$$(3.1) \quad \begin{aligned} A &= \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} \underbrace{a_i \tilde{a}_j}_{x_{ij}} U^i V^j, \\ B &= \sum_{k=1}^{n-1} \sum_{l=1}^{n-1} \underbrace{b_k \tilde{b}_l}_{y_{kl}} U^k V^l \end{aligned}$$

of n^2 equations with $(n-1)^2$ unknowns x_{ij} and y_{kl} . Having a solution of the systems (3.1) one can compute the secret key as follows

$$(3.2) \quad \begin{aligned} K &= P(U, a)P(U, b)P(V, \tilde{a})P(V, \tilde{b}) \\ &= \left(\sum_{i=1}^{n-1} \sum_{j=1}^{n-1} a_i b_j U^{i+j} \right) \left(\sum_{k=1}^{n-1} \sum_{l=1}^{n-1} \tilde{a}_k \tilde{b}_l V^{k+l} \right) \\ &= \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} \sum_{k=1}^{n-1} \sum_{l=1}^{n-1} \underbrace{a_i \tilde{a}_k}_{x_{ik}} \underbrace{b_j \tilde{b}_l}_{y_{jl}} U^{i+j} V^{k+l}. \end{aligned}$$

Solution of a system of n equations with n unknowns using Gauss elimination requires $O(n^3)$ time. Thus solution of the systems (3.1) requires $O(n^6)$ time. Having precomputed values U^i and V^i , for $i = 1, \dots, n-1$, one can perform the step (3.2) in $O(n^7)$ time. So the overall time complexity for this approach is $O(n^7)$.

Further we will describe the second approach based on a linear decomposition attack. The algebra $\mathbb{C}^{n \times n}$ has a structure of a vector space over \mathbb{C} of dimension n^2 . Let \bar{U} be the semigroup generated by U , and let \bar{V} be the semigroup generated by V . A basis of the subspace $\text{Sp}(\bar{U}\bar{V})$ can be effectively constructed as follows. Let

$$\begin{aligned} L_0 &= \{I_n\}, \\ L_1 &= \{U, V\}, \\ &\dots \\ L_i &= \{U^k V^l \mid k, l \in \mathbb{N}, k + l = i\}, \\ &\dots \end{aligned}$$

be the sets of matrices considered as vectors. Define

$$V_i = \text{Sp}(L_0 \cup L_1 \cup \dots \cup L_i),$$

for $i = 0, 1, \dots$, the vector space spanned by the indicated set. We choose a basis $B_0 = \{b_0 = I_n\}$ of V_0 , then extend B_0 to basis B_1 of V_1 , and so on. If for some i_0 we get $B_{i_0} = B_{i_0+1}$, then clearly $B = B_{i_0}$ is a basis of $\text{Sp}(\bar{U}\bar{V})$. By the Cayley-Hamilton theorem one has $i_0 \leq 2n - 2$. In construction of B we only use the Gauss elimination process that is polynomial. Note, that we can do it offline, so we will call this phase the *offline phase*. Let b_0, b_1, \dots, b_r be a basis of $\text{Sp}(\bar{U}\bar{V})$, where $b_i = U^{k_i}V^{l_i}$. Now we are ready to recover the secret key K (*online phase*).

- Since $B \in \text{Sp}(\bar{U}\bar{V})$ we can use the Gauss elimination process to obtain a presentation of B in the form

$$(3.3) \quad B = \sum_{i=0}^r \alpha_i U^{k_i} V^{l_i}, \quad \alpha_i \in \mathbb{C}.$$

- Then we have

$$(3.4) \quad \begin{aligned} \sum_{i=0}^r \alpha_i U^{k_i} A V^{l_i} &= \sum_{i=0}^r \alpha_i U^{k_i} P(U, a) P(V, \tilde{a}) V^{l_i} \\ &= P(U, a) \left(\sum_{i=0}^r \alpha_i U^{k_i} V^{l_i} \right) P(V, \tilde{a}) \\ &= P(U, a) B P(V, \tilde{a}) = K. \end{aligned}$$

Note that a similar protocol by Stickel [15] has been analyzed in [4]. A linear decomposition attack based on the decomposition method has been applied.

Now we will provide a rough estimate for the time complexity of the approach above. Observe that the number of the field operations in Gauss elimination performed on a matrix of size $k \times n^2$ is $O(k^2 n^2)$. A basis of $\text{Sp}(\bar{U}\bar{V})$ consist of at most n^2 elements, so it requires $O(n^2 \sum_{k=1}^{n^2} k^2) = O(n^8)$ time to construct it. Computing α_i in (3.3) by solving a system of linear equations using Gauss elimination requires $O(n^6)$ time. Having precomputed values U^{k_i} and V^{l_i} , for $i = 0, \dots, r$, one can perform the step (3.4) in $O(n^5)$ time. So the offline phase could be done in $O(n^8)$ time, the online phase could be done in $O(n^6)$ time, and the overall time complexity is $O(n^8)$.

REFERENCES

- [1] V. A. Roman'kov, *Algebraic cryptography*, Omsk, Omsk State Dostoevsky University, 2013, 135 pp. (in Russian).
- [2] V. A. Roman'kov, *Cryptanalysis of some schemes applying automorphisms*, Prikladnaya Discretnaya Matematika, 3 (2013), 35–51 (in Russian).
- [3] V. T. Markov, A. V. Mihalyov, A. V. Gribov, P. A. Zolotykh, and S. S. Skazhenik, *Quasigroups and rings in coding and cryptoschemes constructing*, Prikladnaya Discretnaya Matematika, 4 (2012), 35–52 (in Russian).

- [4] V. A. Roman'kov, A. G. Myasnikov, *A linear decomposition attack*, Groups Complexity Cryptology, 7 (2015), 81–94, see also [arXiv:1412.6401v1 \[math.GR\]](#).
- [5] M. Andrecut, *A matrix public key cryptosystem*, preprint, [arXiv:1506.00277v1 \[cs.CR\]](#), 31 May 2015.
- [6] V. A. Roman'kov, *A polynomial time algorithm for the braid double shielded public key cryptosystems*, preprint, [arXiv:1412.5277v1 \[math.GR\]](#), 17 Dec. 2014.
- [7] V. A. Roman'kov, *Linear decomposition attack on public key exchange protocols using semidirect products of (semi)groups*, preprint, [arXiv:1501.01152v1 \[cs.CR\]](#), 6 Jan. 2015.
- [8] X. Wang, C. Xu, G. Li, H. Lin, and W. Wang, *Double shielded public key cryptosystems*, Cryptology ePrint Archive, Report 2014/558, Version 20140718:185200, 2014, 1–14, <https://eprint.iacr.org/2014/558>.
- [9] M. Habeeb, D. Kahrobaei, C. Koupparis, and V. Shpilrain, *Public key exchange using semidirect product of (semi)groups*, In: *ACNS 2013*, volume 7954 of *Lecture Notes Comp. Sc.*, p. 475–486, Springer, 2013.
- [10] D. Kahrobaei, H. T. Lam, and V. Shpilrain, *Public key exchange using extensions by endomorphisms and matrices over a Galois field*, preprint, http://www.sci.ccny.cuny.edu/shpil/semi_galois.pdf.
- [11] B. Tsaban, *The Conjugacy Problem: cryptanalytic approaches to a problem of Dehn*, minicourse, Düsseldorf University, Germany, July–August 2012, http://reh.math.uni-duesseldorf.de/gcgta/slides/Tsaban_minicourses.pdf.
- [12] B. Tsaban, *Polynomial time solutions of computational problems in noncommutative-algebraic cryptography*, Journal of Cryptology, 28 (2015), p. 601–622, see also [arXiv:1210.8114v3 \[cs.CR\]](#).
- [13] B. Tsaban, *Practical polynomial time solutions of several major problems in noncommutative-algebraic cryptography (preliminary announcement)*, IACR eprint 2014/041. Version 20140115:201530, Jan. 2014.
- [14] A. Ben-Zvi, A. Kalka, and B. Tsaban, *Cryptanalysis via algebraic spans*, Cryptology ePrint Archive, Report 2014/041, Version 20150525:211323, 2014, 1–11, <https://eprint.iacr.org/2014/041>.
- [15] E. Stickel, *A New Method for Exchanging Secret Keys*, In: *Proc. of the Third International Conference on Information Technology and Applications (ICITA05)*, 2 (2005), 426–430.

INSTITUTE OF MATHEMATICS AND INFORMATION TECHNOLOGIES, OMSK STATE DOSTOEVSII UNIVERSITY

E-mail address: romankov48@mail.ru

INSTITUTE OF MATHEMATICS AND INFORMATION TECHNOLOGIES, OMSK STATE DOSTOEVSII UNIVERSITY

E-mail address: menshov.a.v@gmail.com